PIA information

PIA
Analise de riscos de GainzCompany

Author's name
João Carvalho

Assessor's name
Carlos Gonçalves

Validator's name
Ricardo Peixoto

Creation date
11/04/2019

DPO's name
João Carvalho

DPO's opinion
Bastantes medidas implementadas para a redução dos riscos

Search of concerned people opinion
Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested
Não se aplica

Context

Overview

Which is the processing under consideration?

Dados recolhidos pela empresa de suplementação alimentar GainzCompany.

What are the responsibilities linked to the processing?

Evitar vazamento e uso abusivo dos dados recolhidos.

Are there standards applicable to the processing?

Não

Evaluation : Acceptable

Data, processes and supporting assets

What are the data processed?

Dados biométricos e dados relacionados com o pagamento e envio de encomendas.

How does the life cycle of data and processes work?

Os dados serão armazenados e processados desde o memonto que o cliente introduz os mesmos na aplicação até os remover da mesma ou terminar a relação comercial com a empresa.

What are the data supporting assets?

Utilizaremos servidores Linux, Base de Dados MongoDB e faremos a aplicação em NodeJS.

Evaluation : Acceptable

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Sim, visto que os dados serão usados para a recomendação de produtos e envio das encomendas.

Evaluation : Acceptable

What are the legal basis making the processing lawful?

Os consumidores aceitam os termos de uso e responsabilidade apresentados no momento de registo na aplicação.

Evaluation : Acceptable

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Sim, apenas recolhemos os dados estritamente necessários para a realização do serviço.

Evaluation : Acceptable

Are the data accurate and kept up to date?

Confiamos na veracidade dos dados introduzidos pelos clientes.

Evaluation : Acceptable

What are the storage duration of the data?

A informação será guardada até o cliente pretender a sua remoção ou até a relação comercial terminar.

Evaluation : Acceptable

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Nos termos de uso e responsabilidade que são apresentados no registo estará o método usado para processar os dados.

Evaluation : Acceptable

If applicable, how is the consent of data subjects obtained?

Através da aceitação dos termos de uso e responsabilidade apresentados

Evaluation : Acceptable

How can data subjects exercise their rights of access and to data portability?

A aplicação terá uma zona que apresenta todos dados relativos aos clientes.

Evaluation : Acceptable

How can data subjects exercise their rights to rectification and erasure?

A aplicação terá uma zona que apresenta todos dados relativos aos clientes e a opção para os mudar ou remover

Evaluation : Acceptable

How can data subjects exercise their rights to restriction and to object?

Os clientes podem optar por não fornecer os dados à aplicação, perdendo algumas funcionalidades que dependeriam desses mesmos dados.

Evaluation : Acceptable

Are the obligations of the processors clearly identified and governed by a contract?

Sim

Evaluation : Acceptable

In the case of data transfer outside the European Union, are the data adequately protected?

Não se aplica

Evaluation : Acceptable

Risks

Planned or existing measures

Comunicação segura

Pretendemos usar metodos que permitam a comunicação segura entre o cliente e os servidores da aplicação

Evaluation : Acceptable

Encryption

Toda a informação relativa aos clientes será cifrada com uma chave que apenas o cliente terá acesso.

Evaluation : Acceptable

Logical access control

- O acesso a uma conta será feito através de um sitema de 2 Factor Authentication, onde será pedida uma password de 8 caractéres (no mínimo) com pelo menos 1 dígito incluído, e também será pedido um código que será enviado para um segundo sistema escolhido pelo utilizador (Email, telemóvel, ...). O acesso a uma conta será restringido após 3 tentativas de autenticação falhadas, sendo que esta apenas só pode ser desbloqueada através de um link que será enviado para uma das opções de contacto da pessoa.

Evaluation : Acceptable

Archiving

Todos os dados serão guardados em servidores locais, e geridos pela empresa

Evaluation : Acceptable

Paper document security

Toda a informação relativa aos clientes pemanecerá em forma digital, ou seja, não serão feitas cópias dessa informação em papel.

Evaluation : Acceptable

Minimising the amount of personal data

A nossa aplicação apenas recolherá a informação minima necessária para a disponibilização de funcionalidades.

Evaluation : Acceptable

Backups

Teremos servidores de backup que terão uma replica dos dados.

Evaluation : Acceptable

Relations with third parties

A informação relativa aos clientes não será partilhada

Evaluation : Acceptable

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

A sua informação pessoal ser revelada

What are the main threats that could lead to the risk?

O uso de cifras já consideradas inseguras., A comunicação entre o servidor e o cliente não ser segura

What are the risk sources?

As cifras usadas para cifrar dados, Os métodos usados para obter uma comunicação segura, As chaves usadas pelos utilizadores

Which of the identified controls contribute to addressing the risk?

Comunicação segura, Encryption, Paper document security, Logical access control

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Caso a informação dos clientes seja vazada seria um risco severo, mas as medidas tomadas conseguem reduzir significativamente esse risco.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, As medidas tomadas reduzem a possíbilidade da ocurrencias de ameaças.

Evaluation : Acceptable

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

Erros em funcionalidades da aplicação ou na informação de compra de produtos

What are the main threats that could lead to the risk?

Erros na base de dados, Vulnerabilidades no Sistema de Autentticação

What are the risk sources?

Alguém que se encontre próximo dos servidores e os danifique, Ataques Direcionados aos servidores / base de dados, Desastres naturais

Which of the identified controls contribute to addressing the risk?

Encryption, Comunicação segura, Backups, Logical access control

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Limited, A modificação da informação que a aplicação obtém não apresenta grande risco para o utilizador e as medidas tomadas ajudam a recuperar de tal acontecimento caso aconteça

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, É pouco provável que este risco ocorra devido as medidas tomadas, como dados cifrados e comunicação segura entre cliente e servidor.

Evaluation : Acceptable

Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

Os utilizadores teriam que preencher novamente os dados pessoais caso pretendam utilizar determinadas funcionalidades novamente

What are the main threats that could lead to the risk?

Catástrofe natural / incêndio, Ataque à base de dados, Falha na Base de dados

What are the risk sources?

Alguém próximo dos servidores (ou base de dados) que danifique o hardware, Catástrofes naturais, Ataques informáticos

Which of the identified controls contribute to addressing the risk?

Logical access control, Comunicação segura, Backups

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible, Alguns riscos não podem ser controlados como catástrofes naturais, mas visto que a aplicação não necessita desta informação para prestar o serviço não será um grande problema se a perdermos. Para além desse risco, as medidas tomadas ajudam a reduzir o efeito (backups).

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, É muito pouco provável que um destes riscos aconteça

Evaluation : Acceptable

Action plan

Overview

Fundamental principles

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Information for the data subjects
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers

Planned or existing measures

Comunicação segura
Encryption
Logical access control
Archiving
Paper document security
Minimising the amount of personal data
Backups
Relations with third parties

Risks

Illegitimate access to data
Unwanted modification of data
Data disappearance

Improvable Measures
Acceptable Measures

Fundamental principles

No action plan recorded.

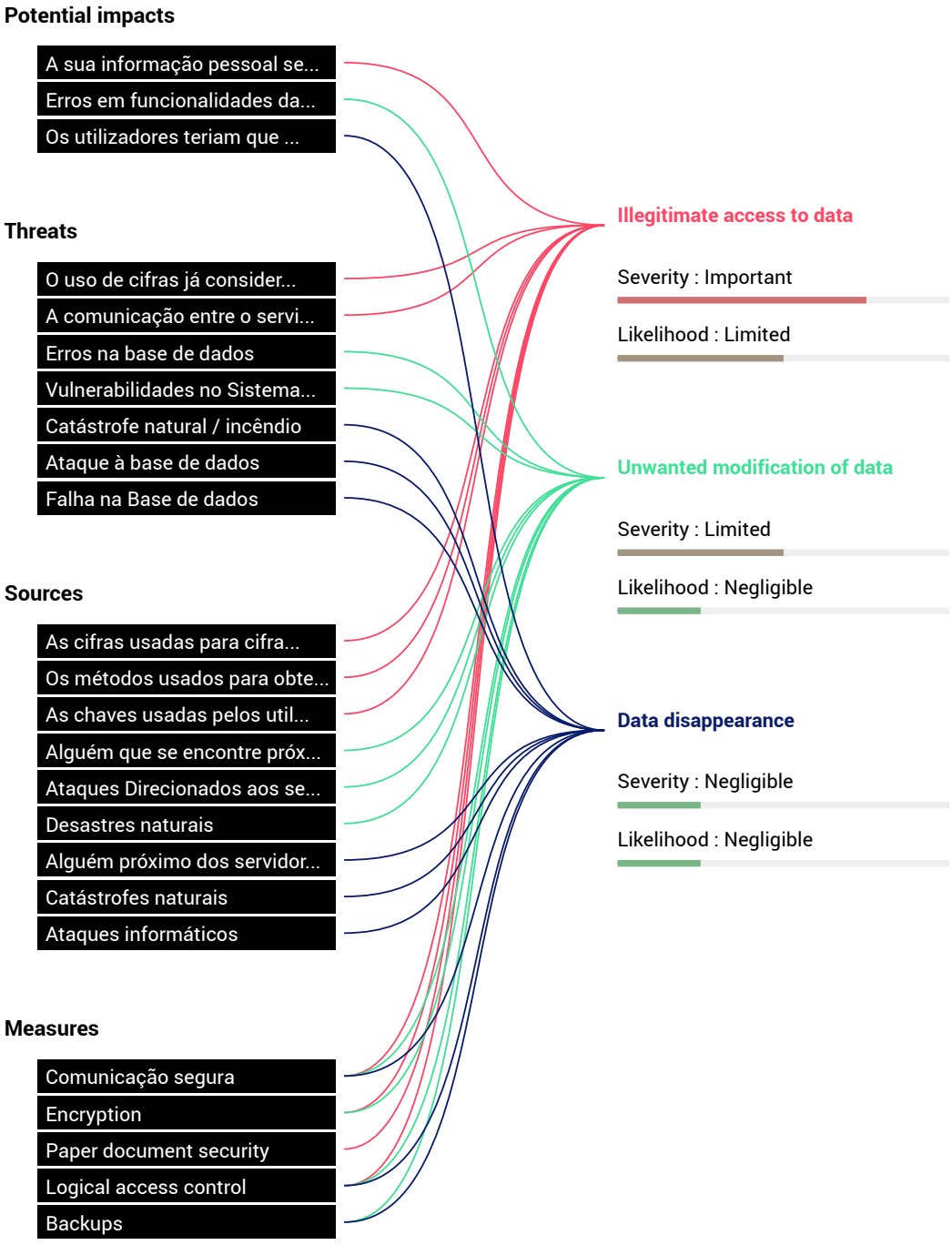
Existing or planned measures

No action plan recorded.

Risks

No action plan recorded.

Risks overview



Risk mapping

- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

11/04/2019